系列のLinear Compexity(離散数理モデルにおける最適組合せ構造)

AUTHOR(S):

今村, 恭己

CITATION:

今村, 恭己. 系列のLinear Compexity(離散数理モデルにおける最適組合せ構造). 数理解析研究所講究録 1993, 820: 59-71

ISSUE DATE:

1993-02

URL:

http://hdl.handle.net/2433/83175

数理解析研究所講究録
第820巻 1993年 59-71

系列の Linear Compexity

九工大情報工学部 今村 恭己 (Kyoki Imamura)

1. はじめに

有限体 $GF(q)$, ($q = p^m$ は素数 p の巾乗), 上の長さ N の系列

$$a_0, a_1, \cdots, a_{N-1} \tag{1}$$

に対して、この系列が満足する $GF(q)$ 上の最小階数の線形定係数差分式

$$a_i = f_1 a_{i-1} + \cdots + f_L a_{i-L} \tag{2}$$

の階数 $L = L(N)$ を系列 (1) の **Linear Complexity (LC)** と呼ぶ [1, 2]。

系列の LC と系列が満足する最小階数の差分式とを求める問題は代数符号の復号の核となる問題であり、その解法としては、$L(1), L(2), \cdots, L(N)$ を効率良く逐次求める Berlekamp-Massey アルゴリズム [3, 4] の他に Euclid の互除法を用いるもの [5] や連分数を用いるもの [6, 7] が知られている。差分式 (2) は系列の連続する $2L$ 個の値から決定される [4, 8] ので、暗号やスペクトル拡散通信の分野では擬似乱数系列（擬似雑音系列）の予測し難さの尺度として LC が用いられる [1, 9]。小さな LC の系列から大きな LC の系列を作る方法も提案されている [10]。周期 T の周期系列 $\{a_i\}$ は差分式 $a_i = a_{i-T}$ を満足するので、その周期系列としての LC, $L = L(\infty)$, は $L \leq T$ である。

本稿では、$L(N)$ が N の関数として特徴のある 3 種類の系列を紹介する。一番目の系列は $GF(q)$ 上の非周期無限長系列であり、系列の LC は N の増加とともに小刻みに、偶数の N に対しては $L(N) = N/2$、奇数の N に対しては $L(N) = (N+1)/2$ のように、増加する。二番目の系列は標数 2 の有限体上の非周期無限長系列であり、$L(N)/N$ の $N \to \infty$ での極限値は存在せず、区間 $[1/3, 2/3]$ の任意の値を取る。三番目の系列は $GF(q)$ 上の m- 系列と呼ばれる周期 $T = q^n - 1$ の周期系列から最小の変更により得られる同じ周期の T 個の周期系列であり、次のような特徴を持つ。先ず $GF(q)$ 上の周期 T の m- 系列 $\{a_i\}$ から同じ周期の周期系列 $\{b_i^{(j)}\}, (0 \leq j \leq T)$, を $b_i^{(j)} = a_i + b$ $(\text{if } i \equiv j \ mod\ T), (b \in GF(q) \setminus \{0\})$, $b_i^{(j)} = a_i$ (otherwise) により得ることを m- 系列 $\{a_i\}$ の最小の変更と呼ぶ。b を固定すると j の値に対応して T 個の系列 $\{b_i^{(j)}\}$ が得られるが、その LC は、唯一つの $j = j(b)$ に対して $T-n$ となるがその他の j では T となる。これは周期 $T = q^n - 1$ の周期系列の中で最小の LC を持つ m- 系列から最小の変更により得られる T 個の系列は 1 つを除き皆最大の LC を持つことを意味する。

これら 3 つの系列は、擬似乱数系列の予測し難さとか乱数らしさの尺度としての LC の弱点を示唆する系列の典型的な例になっている。

2. 系列 I

$GF(q)$ 上の非周期無限長系列 $\{a_i\}$, $(i \geq 0)$, を

$$a_i = \begin{cases} b_k \neq 0 & \text{if } i = 2^k - 1, \\ 0 & \text{otherwise} \end{cases} \tag{3}$$

により定義する。この系列の LC については次の定理が成り立つ。

[**定理 1**]

$$L(N) = \begin{cases} N/2 & (N\text{: 偶数}), \\ (N+1)/2 & (N\text{: 奇数}). \end{cases} \tag{4}$$

このことは、$q = 2$ の場合について、Rueppel[11] により予想され、Dai[12] と著者等 [13] により証明された。ここでは、著者等 [13] の証明を紹介する。系列長の増加とともに LC が (4) のように増加する系列が最も望ましい擬似乱数系列であると予想されている [1] が、この系列のように極めて簡単な規則で生成されるものが (4) を満足することは興味深い。

以下で述べる証明では、Berlekamp-Massey アルゴリズム [3, 4] に関する次の 2 つの性質 [8] を用いる。

[**補題 1**] $L(2m) = m$ であるための必要十分条件は、$m \times m$ の Hankel 行列

$$A(m) = \begin{bmatrix} a_0 & a_1 & \dots & a_{m-1} \\ a_1 & a_2 & \dots & a_m \\ \dots & \dots & \dots & \dots \\ a_{m-1} & a_m & \dots & a_{2m-2} \end{bmatrix} \tag{5}$$

が正則であることである。

[**補題 2**] $N=2m$ と $N=2m'$, $(m<m')$, とを $L(N)=N/2$ となる隣合う N の値とすると、$L(N)$ は区間 $[2m, 2m']$ においてその中央の点 $N=m+m'$ でのみ増加し、その増分量はこの区間の長さの半分に等しい。差分式 (2) は、$L(N) \leq N/2$ の場合にのみ一意である。

定理 1 の証明： 補題 1, 2 により、系列 (3) を (5) に代入して作られる Hankel 行列 $A(m)$ が全ての非負整数 m に対して正則であることを示せば良い。これは m に関する数学的帰納法により示すことが出来る。

先ず $m=1=2^0$ と $m=2=2^1$ の場合は、$A(m)$ は正則である。次に $m \leq 2^{k-1}$ に対しては $A(m)$ が正則であると仮定すれば、$2^{k-1}<m \leq 2^k$ についても $A(m)$ が正則であることは、

$$A(m)=\left[\begin{array}{c|c} A(2^{k-1}) & B \\ \hline B^T & 0 \end{array}\right], \tag{6}$$

ただし B^T は B の転置行列であり、

$$B=\left[\begin{array}{c} 0 \\ \hline b_k E(m-2^{k-1}) \end{array}\right], \tag{7}$$

$$E(m-2^{k-1})=\begin{bmatrix} 0 & \ldots & 0 & 1 \\ 0 & \ldots & 1 & 0 \\ \multicolumn{4}{c}{\cdots\cdots\cdots} \\ 1 & \ldots & 0 & 0 \end{bmatrix} \tag{8}$$

（逆対角行列）と $b_k \neq 0$ とにより明らかである。

Q.E.D.

3. 系列 II

標数 2 の有限体 $GF(q)$ 上の非周期無限長系列

$$a_0, a_1, a_2, \ldots, \tag{9}$$

を無限長の連分数

$$F(x) = \cfrac{1}{x^{2^0} + \cfrac{1}{x^{2^1} + \cfrac{1}{x^{2^2} + \cfrac{1}{x^{2^3} + \ddots}}}} \tag{10}$$

を用いて次のように定義する。$F(x)$ を x^{-1} の巾級数に展開したときの x^{-i} の係数が a_{i-1} である。

$$F(x) = a_0 x^{-1} + a_1 x^{-2} + a_2 x^{-3} + \ldots \tag{11}$$

この系列については次の定理が成り立つ。

[**定理 2**] この系列の LC は、$3 \times 2^{i-1} - 2 \leq N \leq 3 \times 2^i - 3$ に対して $L(N) = 2^i - 1$ となり、$\lim_{N\to\infty} L(N)/N$ は振動し区間 $[1/3, 2/3]$ の任意の値を取る。

[**定理 3**] この系列の一般項は次のように決定される。先ず $a_0 = 1, a_1 = 0$ を初期値として、先頭の 2^{i-1} 項迄が求まったとすれば、先頭の 2^i 項の後半の 2^{i-1} 項 $a_{2^{i-1}}, \ldots, a_{2^i-1}$ は、前半分の 2^{i-2} 項を全て 0 とし、後半分の 2^{i-2} 項を系列 $\{a_i\}$ の先頭の 2^{i-2} 項 $a_0, \ldots, a_{2^{i-2}-1}$ に等しく置けば良い。

連分数 (10) を最初の i 項迄で打切ったものを既約な多項式の組 $\{P_i(x), Q_i(x)\}$ (Q_i の最高次の係数は 1) の比として

$$\frac{P_i}{Q_i} = \cfrac{1}{x^{2^0} + \cfrac{1}{x^{2^1} + \cfrac{1}{x^{2^2} + \ddots + \frac{1}{x^{2^{i-1}}}}}} \tag{12}$$

と書くと、$\{P_i(x), Q_i(x)\}$ は初期値 $Q_0 = 1, P_0 = 0, Q_1 = x, P_1 = 1$ から出発して漸化式 $Q_{i+1} = x^{2^i} Q_i + Q_{i-1}, P_{i+1} = x^{2^i} P_i + P_{i-1}$ により求まるので $deg\, Q_i = 2^i - 1, deg\, P_i = 2^i - 2$ である。

系列の LC と差分式 (2) とを求めるための連分数を用いる解法についての性質 [6] から次の補題が成り立つ。

[**補題 3**]

$$\frac{P_i}{Q_i} = b_0 x^{-1} + b_1 x^{-2} + b_2 x^{-3} + \ldots \tag{13}$$

と書くとき、$0 \leq k \leq deg\, Q_i + deg\, Q_{i+1} - 2$ については $b_k = a_k$ であり、$k = deg\, Q_i + deg\, Q_{i+1} - 1$ においては $b_k \neq a_k$ である。系列 (8) の LC, $L(N)$, は $deg\, Q_1, deg\, Q_2, \ldots$ の値を順に取り、$deg\, Q_{i-1} + deg\, Q_i \leq N \leq deg\, Q_i + deg\, Q_{i+1} - 1$ の区間で $L(N) = deg\, Q_i$ となる。

この補題 3 と $deg\, Q_i = 2^i - 1$ とから定理 2 は明らかである。

定理3の証明は、つぎのようにして行なえる。式(12)の形と P_i, Q_i の漸化式とにより、

$$\begin{aligned}\frac{P_i}{Q_i} &= \frac{x^{2^{i-1}}P_{i-1}+P_{i-2}}{x^{2^{i-1}}Q_{i-1}+Q_{i-2}}\\ &= \frac{1}{x+\frac{P_{i-1}(x^2)}{Q_{i-1}(x^2)}}\\ &= \frac{Q_{i-1}(x^2)}{xQ_{i-1}(x^2)+P_{i-1}(x^2)}\\ &= \frac{[Q_{i-1}(x)]^2}{x[Q_{i-1}(x)]^2+[P_{i-1}(x)]^2} \qquad (14)\end{aligned}$$

を得る。次数の関係と上式とにより

$$\frac{P_i}{Q_i} = \frac{Q_{i-1}^2}{x^{2^{i-1}}Q_{i-1}+Q_{i-2}} \qquad (15)$$

と書ける。補題3により

$$\frac{x^{2^i}P_i}{Q_i} = a_0x^{2^i-1}+\cdots+a_{2^i-1}+o(x^{-1}) \qquad (16)$$

であるので、(13)と(15)とにより、

$$\begin{aligned}\frac{x^{2^i}P_i}{Q_i} &= \frac{x^{2^i}Q_{i-1}^2}{x^{2^{i-1}}Q_{i-1}+Q_{i-2}}\\ &= x^{2^{i-1}}Q_{i-1}+Q_{i-2}+\frac{Q_{i-2}^2}{x^{2^{i-1}}Q_{i-1}+Q_{i-2}}\\ &= a_0x^{2^i-1}+\cdots+a_{2^i-1}+o(x^{-1}) \qquad (17)\end{aligned}$$

を得る。この式から

$$\left[\begin{array}{cccc} a_0 & a_1 & \ldots & a_{2^i-1}\end{array}\right] = \left[\begin{array}{c|ccc|c} \overrightarrow{Q_{i-1}} & 0 & \cdots & 0 & \overrightarrow{Q_{i-2}}\end{array}\right] \qquad (18)$$

の関係を得る。ただし $\overrightarrow{Q_{i-1}}$ は多項式 $Q_{i-1}(x)$ の 2^{i-1} 個の係数を最高次の係数を左端におき降巾の順に並べたものである。$Q_1 = x = 1 \cdot x + 0$ に注意すれば、定理 3 を得る。

式 (14) の変形において $P(x^2) = [P(x)]^2$ の関係を用いているので、定理 3 は q が 2 の巾乗の場合に限られる。

4. 系列 III

最後の系列は、$GF(q)$ 上の周期 $T = q^n - 1$ の m- 系列

$$a_i = tr(\alpha^i) \tag{19}$$

(α は $GF(q^n)$ の原始元、$tr(\ )$ は $GF(q^n)$ から $GF(q)$ へのトレースであって $\beta \in GF(q^n)$ に対して $tr(\beta) = \beta^{q^0} + \beta^{q^1} + \cdots + \beta^{q^{n-1}} \in GF(q)$) から最小の変更により得られる T 個の同じ周期の周期系列

$$b_i^{(j)} = \begin{cases} a_j + b, & \text{if } i \equiv j \mod T \\ a_i & \text{otherwise} \end{cases} \tag{20}$$

(ただし $b \in GF(q) \setminus \{0\}, 0 \leq j \leq T-1$) である。

式 (19) の m- 系列 $\{a_i\}$ の周期系列としての LC, $L = L(\infty)$, は $L = n$ であり、これは周期 $T - q^n - 1$ のけいれつの LC の最小値であることとか、T 個の長さ n の状態ベクトル $[a_i, a_{i+1}, \ldots, a_{i+n-1}]$, $(0 \leq i \leq T-1)$ は全て相異なり零ベクトル以外の全てのベクトルが 1 回ずつ出現すること等は良く知られている。周期 T の周期系列の周期系列としての LC は、第 1 節で述べたように、$L = L(\infty) \leq T$ であるので、補題 2 を考慮すると $L = L(2T)$ である (もしも $L(2T) < L$ とす

れば、$L(N)$ は $N > 2T$ において少なくとも 1 回は増加するが、その結果は、補題 2 により、$L > T$ となる）。

周期系列 (20) の周期系列としての LC を L_j, $(0 \leq j \leq T-1)$, と書き、変更量 $b \in GF(q)$ を

$$b = \alpha^{uT/(q-1)}, \quad 0 \leq u \leq q-2 \tag{21}$$

と書くと、次の定理 [14] が成り立つ。

[**定理 4**] 系列 (20) の LC, L_j, は、

$$L_j = \begin{cases} T-n & \text{if } j = uT/(q-1), \\ T & \text{otherwise} \end{cases} \tag{22}$$

であり、1 つの j を除き、L_j は最大値を取る。

この結果は、m- 系列のような LC の小さい系列から大きな LC を持つ系列を作る試み [10] に対する注意という意味で著者等 [14] により提示された。

定理 4 の証明 [15]： 補題 1, 2 と $L_j \leq T, \quad L_j = L(2T)$ とにより、L_j は $T \times T$ Hankel 行列

$$B_j = \begin{bmatrix} b_0^{(j)} & b_1^{(j)} & \dots & b_{T-1}^{(j)} \\ b_1^{(j)} & b_2^{(j)} & \dots & b_T^{(j)} \\ \dots\dots\dots\dots\dots\dots \\ b_{T-1}^{(j)} & b_T^{(j)} & \dots & b_{2T-2}^{(j)} \end{bmatrix} \tag{23}$$

の階数に等しい。

$$L_j = rank \quad B_j. \tag{24}$$

$T \times T$ 巡回行列 C_j, $(0 \leq j \leq T-1)$, を (8) の行列 $E(j+1)$ を用いて

$$C_j = E(j+1) \oplus E(T-j-1) \tag{25}$$

（記号 $\oplus$ は行列の直和を意味する）で定義すると、B_j は (20) により

$$B_j = a_0 E_0 + a_1 E_1 + \cdots + a_{T-1} E_{T-1} + b E_j \tag{26}$$

と書ける。行列 B_j の階数を計算する代わりに B_j を正則な $T \times T$ Vandermonde 行列

$$\begin{aligned} M &= [\alpha^{uv}] \\ &= \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{T-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(T-1)} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & \alpha^{T-1} & \alpha^{2(T-1)} & \cdots & \alpha^{(T-1)(T-1)} \end{bmatrix} \end{aligned} \tag{27}$$

とその逆行列 $M^{-1} = [-\alpha^{-uv}]$ とを用いて変換した行列 $\widehat{B}_j = M B_j M^{-1}$ の階数を計算する。

$$MC_jM^{-1} = 1 \oplus \begin{bmatrix} 0 & \cdots & 0 & \alpha^j \\ 0 & \cdots & \alpha^{2j} & 0 \\ \cdots & \cdots & \cdots & \cdots \\ \alpha^{(T-1)j} & \cdots & 0 & 0 \end{bmatrix} \tag{28}$$

と (26) とにより

$$B_j = b_j(\alpha^0) \oplus \begin{bmatrix} 0 & \dots & 0 & b_j(\alpha^1) \\ 0 & \dots & b_j(\alpha^2) & 0 \\ \dots & \dots & \dots & \dots \\ b_j(\alpha^{(T-1)j}) & \dots & 0 & 0 \end{bmatrix} \tag{29}$$

をうる。ただし

$$\begin{aligned} b_j(x) &= \sum_{0 \le i \le T-1} a_i x^i + b \cdot x^j \\ &= \sum_{0 \le i \le T-1} \sum_{0 \le k \le n-1} \alpha^{iq^k} x^i + b \cdot x^j. \end{aligned} \tag{30}$$

したがって

$$b_j(\alpha^u) = \begin{cases} (b\alpha^{-j} - 1)^{q^k} & \text{if } u = T - q^k, \quad 0 \le k \le n-1, \\ b\alpha^{uj} & \text{otherwise} \end{cases} \tag{31}$$

により定理 4 を得る。

Q.E.D.

5. むすび

系列の LC は、簡単な計算法が知られていることと簡単なデジタル回路 (LC に等しい段数の LFSR (Linear Feedback Shift Register)) で系列を生成出来ることとにより、系列の complexity (予測し難さ、乱数系列らしさ) の便利な評価法として従来から多用されている。

本稿で示した 3 つの系列は、系列の complexity の評価尺度としての LC の弱点を直観的に示唆する系列の典型的な例に

なっている。これらの系列を別の評価法で検討し比較することは興味深い。

参考文献

[1] R. A. Rueppel,*Analysis and Design of Stream Ciphers*, Heidelberg, Springer-Verlag, 1986.

[2] J. L. Massey, "An introduction to contemporary cryptology", *Proc. IEEE*, vol. 76, pp. 533-549, May 1988.

[3] E. R. Berlekamp, *Algebraic Coding Theory*, New York, McGraw- Hill, 1968.

[4] J. L. Massey, "Shift register synthesis and BCH decoding", *IEEE Trans. Inform. Theory*, vol. IT-15, pp. 122-127, Jan. 1969.

[5] Y. Sugiyama, M. Kasahara, S. Hirasawa and T. Namekawa, " A method for solving key equation for decoding Goppa codes", *Inform. Contr.*, vol. 27, pp. 87-99, Jan. 1975.

[6] W. H. Mills, "Continued fractions and linear recurrences", *Math. Comp.*, vol. 29, pp. 173-180, 1975.

[7] R. A. Scholtz and L. R. Welch, "Continued fractions and Berlekamp's algorithm", *IEEE Trans. Inform. Theory*, vol. IT-25, pp. 19-27, Jan. 1979.

[8] K. Imamura and W. Yoshida, "A simple derivation of the Berlekamp-Massey algorithm and some applications", *IEEE Trans. Inform. Theory*, vol. IT-33, pp. 146-150, Jan. 1987.

[9] M. K. Simon, J. K. Omura, R. A. Scholtz and B. K. Levitt, *Spread Spectrum Communications*, vol. I, Chap. 5, Computer Science Press, 1985.

[10] I. Vajd and T. Nemetz, "Substitution ofcharacters in q-ary m-sequences", in Sakata (ed.), *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, pp. 96-105, Heidelberg, Springer-Verlag, 1991.

[11] R. A. Rueppel, "Linear complexity and randomsequences", *Proc. EUROCRYPT '85*, pp. 167-188, Springer-Verlag, 1985.

[12] Z. Dai, "Proof of Rueppel's linear complexity conjecture", *IEEE Trans. Inform. Theory*, vol. IT-32, pp. 440-443, May 1986.

[13] K. Imamura, W. Yoshida and M. Morii, "Two binary sequences and their linear complexities", *Abst. IEEE 1988 Intern. Symp. Inform. Theory*, pp. 216-217, June 1988.

[14] K. Imamura, T. Moriuchi and S. Uehara, "Periodic sequences of the maximum linear complexity simply obtained from an m-sequence", *Proc. IEEE 1991 Intern. Symp. Inform. Theory*, p. 175, June 1991.

[15] K. Imamura and G. Xiao, "On periodic sequences of the maximum linear complexity and m-sequences", to be presented at the *IEEE ICC/ISITA '92*, Singapore, Nov. 16-20, 1992.